(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 October 2001 (04.10.2001)

PCT

(10) International Publication Number
WO 01/73530 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/US01/09631

(22) International Filing Date: 26 March 2001 (26.03.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/536,203 27 March 2000 (27.03.2000) US

(71) Applicant: SECURIT-E-DOC, INC. [US/US]: 1689 Forum Place, West Palm Beach, FL 33401 (US).

(72) Inventor: BARRON, Robert, H.; 1025 Morse Blvd., Singer Island, FL 33404 (US).

(74) Agent: SLAVIN, Michael; McHale & Slavin, P.A., 4440 PGA Blvd., Suite 402, Palm Beach Gardens, FL 33410 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 01/73530 A2

(54) Title: METHOD, APPARATUS, AND SYSTEM FOR SECURE DATA TRANSPORT

(57) Abstract: A platform allowing for the secure file transfer from one location to another (internet or intranet) with virtually impregnable encryption, secure data storage, and a simple web-based user interface. A user accesses the system by a data-base authentication system requiring user name and password. The program residing on the server then generates an encryption sequence. A temporary file is created on the users' machine upon which the user uploads the information to be sent. The information is automatically encrypted by the program and transferred to the server and the user's temporary file deleted. The information is securely stored in the program on the server until the recipient downloads it. The recipient also accesses the server by a user name and password. The program generates a decryption program. The recipients machine receives the applet program to decrypt the file and a copy of the encrypted file. After decryption is complete, the program saves the files to a specified recipient folder, and can be automatically deleted or archived.

The interconnected computers exchange information using various services, for example, the World Wide Web (WWW) and electronic mail. The WWW created a way for computers in various locations to display text that contained links to other files. The WWW service allows a server computer system (Web server or Web site) to send graphical Web pages of information to a remote client computer system. The remote client computer system can then display the Web pages.

In a standard e-mail system, a user's computer is connected to a provider of Internet services, and the user's computer provides an e-mail password when polling the provider's computer for new mail. The mail resides on the provider's computer in plain text form where it can be read by anyone. In both examples, the information, if unsecured, is replicated at many sites in the process of being transmitted to a destination site and thereby is made available to the public.

Organizations are increasingly utilizing these networks, to improve customer service and streamline business communication through applications such as e-mail, messaging, remote access, intranet based applications, on-line support and supply chain applications. The very openness and accessibility that has stimulated the use of public and private networks has also driven the need for network security.

Presently, to provide for a secure transfer of information, it may be encrypted at the sending host's end and decrypted at the receiver's end. Encryption algorithms transform written words and other kinds of messages so that they are unintelligible to unauthorized recipients. An authorized recipient can then transform the words or messages back into a message that is perfectly understandable. Currently, there are two basic kinds of encryption algorithms (1) symmetric key

encryption keys from passphrases. For example, Pretty Good Privacy (PGP) uses message digests to transform a passphrase provided by a user in to an encryption key that is used for symmetric encryption. (PGP uses symmetric encryption for its "conventional encryption" function as well as to encrypt the user's private key). A few digest in use are HMAC, MD2, MD4, MD5, SHA, and SHA-1.

Working cryptographic systems can be divided into two categories; (1) programs and protocols that are used for encryption of e-mail messages such as PGP and S/MIME and (2) cryptographic systems used for providing confidentiality, authentication, integrity, and nonrepudiation in a network environment. The latter requires real-time interplay between a client and a server to work properly. Examples include Secure Socket Layer (SSL) a general-purpose cryptographic protocol that can be used with any TCP/IP service and PCT a transport layer security protocol for use with TCP/IP service, PCT, S-HTTP, SET, Cybercash, DNSSEC, Ipsec, IPv6, Kerberos, and SSH.

Although the present means of securing the electric transfer of information provides a level of security, the security provided can be easily breached. Symmetric encryption algorithms are vulnerable to attack by (1) key search or brute force attacks, (2) cryptanalysis, and (3) systems-based attacks. First, in a key search, the cracker simply tries every possible key, one after another, until the he/she is allowed into the system or the ciphertext is decrypted. There is no way to defend against this but a 128 bit key is highly resistant because of the large number of possible keys to be tried.

Second, in cryptanalysis, the algorithm can be defeated by using a combination of sophisticated mathematics and computer power. Many encrypted messages can be deciphered without knowing the key. Finally, the

apparatus for encrypting data with a either a random automatic mode of encryption, and a client selected private key, that does not travel with the document. The method and apparatus, writes the encryption algorithm creating a packaged application. The encryption program generates random sequences or encryption algorithms, with respect to time sensitivity, to be used in the packaged application that it creates. No two algorithms will ever be the same.

In the basic embodiment, the client accesses the server using a data-base authentication system requiring User name and Password. Once access is granted, the packaged application is sent to the client machine as a temporary file to encrypt the files being sent or uploaded to the server. The application package breaks the files down into binary form, reads the binary form, and then rewrites the data to the temporary file it created. On a binary level, the code is rewritten and saved for transfer in a file format only decodable by the end recipient. Once this process is complete, the application packet then sends the encrypted data to the server via SSL protocol connection.

The data resides on the server waiting for an intended recipient to download and unlock it. When file retrieval is requested, the server authenticates the user and password via a log-on system. Once access is granted, the server generates a new application packet designed to decrypt the file being requested, based on the original encryption algorithm. The server retrieves its original entry, sets into motion the sequence of creating a decryption program, saves the generated program, and then sends the application packet to the requesting client machine.

The client machine receives the application packet to decrypt the file from the server and a copy of the file to

finger print scanner, smart card reader or the like anc be implemented in order to send or retrieve information.

Yet another objective of the instant invention is to provide virtually impregnable security for the delivery, storage, and sharing of documents and files utilizing any compatible network as a secure communications forum.

Other objects and advantages of this invention will become apparent from the following description taken in conjunction with the accompanying drawings wherein are set forth, by way of illustration and example, certain embodiments of this invention. The drawings constitute a part of this specification and include exemplary embodiments of the present invention and illustrate various objects and features thereof.

BRIEF DESCRIPTION OF THE FIGURES

Figure **1** is a block diagram of the client file encryption transfer request of the instant invention;

Figure **2** is a block diagram of the encryption transfer;

Figure **3** is a block diagram of the recipient file request; and

Figure **4** is a block diagram of the decryption transfer.

DETAILED DESCRIPTION OF THE INVENTION

Although the invention will be described in terms of a specific embodiment, it will be readily apparent to those skilled in this art that various modifications, rearrangements, and substitutions can be made without departing from the spirit of the invention. The scope of the invention is defined by the claims appended hereto.

Now, referring to Fig. **1**, shown is flow chart depicting the steps required for encrypting data allowing for secure transfer of electronic data. A client **10** opens

generated sequence specified by the particular and customized applet. The sequence is also designed to replace every other matching bit of binary code with a unique string. Thus, with this method, an "a", for example, will never be represented twice in the same file structure. This is designed to deter the common method of cracking encrypted code by repeated or pattern data. On a binary level, the code is rewritten and saved for transfer in a file format only decodable by the recipient. The applet then sends the encrypted data to the server via SSL protocol. Once the transfer is complete, the applet deletes any trace of the file encrypted. With the destruction of the applet, no two applications are ever the same because each application contains it's own encryption sequence that cannot be replicated.

The encrypted data resides on the server **12** waiting for an intended recipient to download and unlock it. This creates the ability to maintain completely encrypted and secure data archives. When file retrieval is requested by a recipient, the server then accesses the original record information of the sequence or algorithm that it originally gave to the applet that the server created to encrypt the file.

Now referring to Fig. **3**, shown is the flow chart depicting the steps for decrypting data for a secure receipt of electronic data. A recipient **50** opens a web browser and accesses a qualified server **12** therein requesting data transfer. The server **12** provides login account qualifier data requiring either user name and a password **52** or a biometric interface **54** such as a retinal scanner, finger print scanner, smart card reader and the like for the purpose of seeking data-base authentication **56**. If login fails, the user has three attempts **58** before the account is locked **60** and the administrator and the account holder **62** is alerted.

CLAIMS

What is claimed is:

Claim 1. A method of encrypting data for secure transfer and storage of electronic data comprising the steps of:

accessing a conventional web browser;

logging onto a qualified server and providing account qualifier data;

reading a transfer information inquiry page upon verification of account qualifier;

obtaining a first applet compiled on said server in response to said inquiry page, said first applet used to create a temporary file for the upload of data;

submitting a file for encryption to said applet;

encrypting said file and forming an encrypted data packet;

forwarding said data packet to said qualified server for storage;

providing a means for decrypting said encrypted data packet.

Claim 2. The method according to claim 1 wherein said account qualifier is a user name and password.

Claim 3. The method according to claim 1 wherein said account qualifier is a smart card reader.

Claim 4. The method according to claim 1 wherein said account qualifier is a biometric interface.

Claim 5. The method according to claim 4 wherein said biometric interface is a retinal scanner.

Claim 13. The method according to claim 1 wherein said account qualifier is compared against a stored database.

Claim 14. The method according to claim 1 said encrypting of said file occurs during a transfer to said server.

Claim 15. A method of encrypting data for secure transfer and storage of electronic data comprising the steps of:

accessing a conventional web browser;

logging onto a qualified server and providing account qualifier data;

reading a transfer information inquiry page upon verification of account qualifier;

obtaining a first applet compiled on said server in response to said inquiry page, said first applet used to create a temporary file for the upload of data;

submitting a file for encryption to said applet;

encrypting said file and forming an encrypted data packet;

forwarding said data packet to said qualified server for storage and destroying said first applet;

obtaining a second applet compiled on said server in response to said inquiry page, said second applet used to create a temporary file for the download of said encrypted data;

decrypting said file and destroying said second applet.

Claim 16. The method according to claim 15 wherein said account qualifier is a user name and password.

decrypt said data file, said second applet allowing for the downloading and decryption of said data file.

Claim 25. The system according to claim 24, wherein said applets are controlled by a user name and password.

Claim 26. The system according to claim 24, wherein said sender selects a secondary private key to layer said encryption.

Claim 27. The system according to claim 26, wherein said secondary key is a digital file lock.

Claim 28. The system according to claim 26, wherein said secondary key biometric interface.

Claim 29. The system according to claim 24 wherein the recipient is notified of an encrypted data file by an e-mail message generated by said system and directed to said recipient.

Claim 30. The system according to claim 29 wherein said e-mail is sent by SSL protocol.

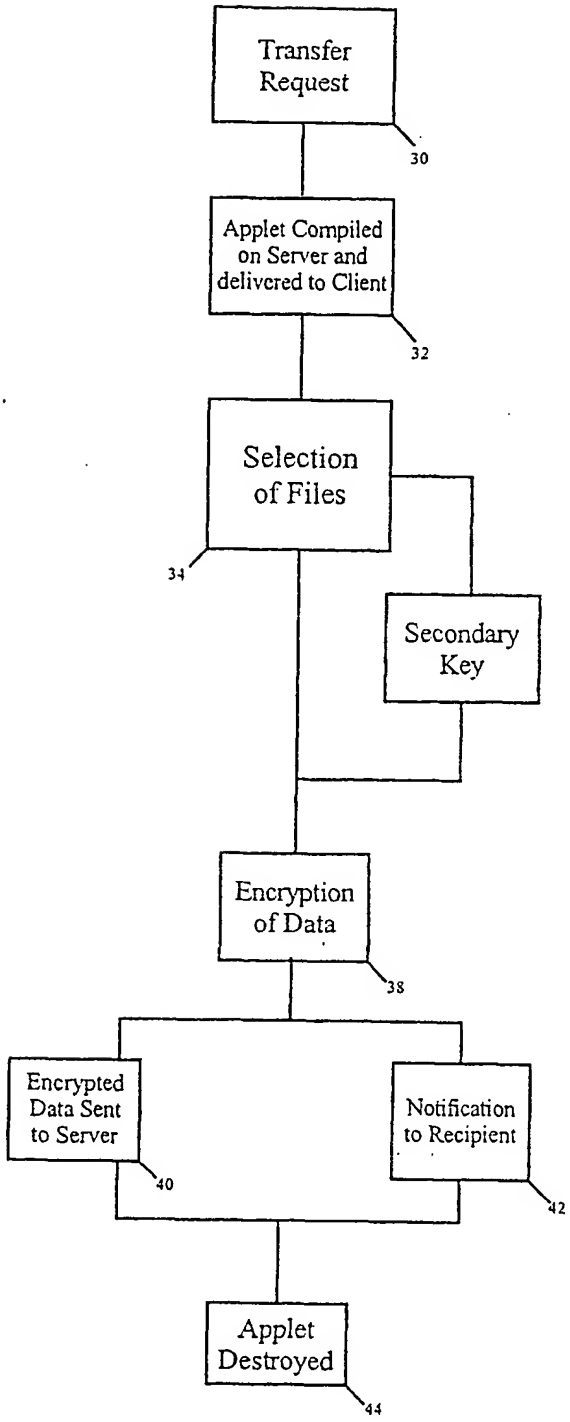
Transfer Request
30
Applet Compiled on Server and delivered to Client
32
Selection of Files
34
Secondary Key
Encryption of Data
38
Encrypted Data Sent to Server
40
Notification to Recipient
42
Applet Destroyed
44

Fig 2

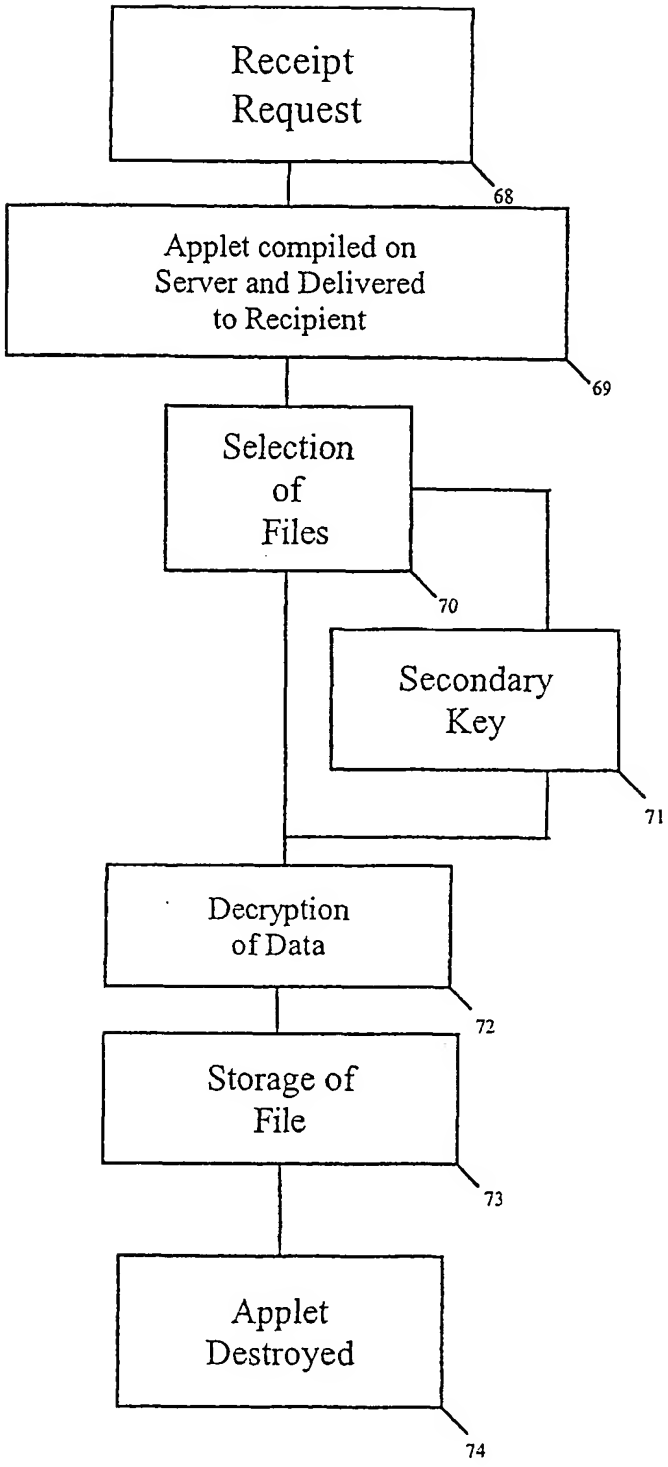
Receipt Request
68
Applet compiled on Server and Delivered to Recipient
69
Selection of Files
70
Secondary Key
71
Decryption of Data
72
Storage of File
73
Applet Destroyed
74

Fig 4.